

Hintergrundinformationen:

Home / Produktfinder 

# Kleines Internet-ABC

## Administrator

[ARP](#)[Bridge](#)[Broadcast](#)[Client](#)[Client-Server-Architektur](#)[Com-Server](#)[DHCP](#)[DNS](#)[DNS Server](#)[Ethernet](#)[Ethernet-Adresse](#)[Firewall](#)[FTP](#)[Gateway](#)[ICMP](#)[Internet](#)[Intranet](#)[IP](#)[IP-Adresse](#)[ISDN](#)[ISDN-Router](#)[LAN](#)[MAC ID](#)[NAT](#)[Ping](#)[PPP](#)[RIP](#)[Router](#)[Server](#)[SLIP](#)[SLIP-Router](#)[SNMP](#)[Subnet-Mas](#)[TCP](#)[TCP/IP-Stack](#)[Telnet](#)[TFTP](#)[UDP](#)

## Administrator

Systemverwalter, der im lokalen Netzwerk uneingeschränkte Zugriffsrechte hat und für die Verwaltung und Betreuung des Netzwerks zuständig ist. Der Administrator vergibt unter anderem die [IP-Adressen](#) in seinem Netzwerk und muß die Einmaligkeit jeder IP-Adresse gewährleisten.

## ARP - Address Resolution Protocol

Über ARP wird die zu einer [IP-Adresse](#) gehörende [Ethernet-Adresse](#) eines Netzwerkteilnehmers ermittelt. Die ermittelten Zuordnungen werden auf jedem einzelnen Rechner in der ARP-Tabelle verwaltet. In Windows-Betriebssystemen kann man auf die ARP-Tabelle mit Hilfe des ARP-Befehls Einfluß nehmen.

Eigenschaften und Parameter des ARP Kommandos in der DOS-Box:

ARP -A listet die Einträge der ARP-Tabelle auf

ARP -S <IP-Adresse> <Ethernet-Adresse> fügt der ARP-Tabelle einen statischen Eintrag hinzu

ARP -D <IP-Adresse> löscht einen Eintrag aus der ARP-Tabelle

ARP ist im Internet-Standard RFC-826 definiert.

## Bridge

Bridges verbinden Teilnetze miteinander und entscheiden anhand der [Ethernet-Adresse](#), welche Pakete die Bridge passieren dürfen und welche nicht. Die dazu notwendigen Informationen entnimmt die Bridge Tabellen, die je nach Modell vom [Administrator](#) eingegeben werden müssen oder von der Bridge dynamisch selbst erstellt werden.

vgl. auch [Router](#)

## Broadcast

Als Broadcast bezeichnet man einen Rundruf an alle Netzteilnehmer. Eine typische Broadcast-Anwendung ist der [ARP-Request](#). Auch andere Protokolle - etwa [RIP](#) - nutzen Broadcast-Meldungen.

Broadcast-Meldungen werden nicht über [Router](#) oder [Bridges](#) weitergegeben.

## Client

Anwendungen, welche Verbindungen zu sogenannten [Servern](#) aufbauen, um die entsprechenden Dienste zu nutzen. Der bekannteste Client ist der Web-Browser, welcher die Verbindung zu einem Web-Server aufnimmt. Praktisch alle Internet-Dienste, wie Mail, [FTP](#), [Telnet](#), Socket usw. arbeiten nach dem Client-Server Schema.

Der Client ist quasi der "Anrufer", während der Server auf "Anrufe" wartet, um diese bei Bedarf anzunehmen.

## Client-Server-Architektur

System der "verteilten Intelligenz", bei dem der [Client](#) Verbindung zu einem [Server](#) aufbaut, um vom Server angebotene Dienste in Anspruch zu nehmen. Manche Server-Anwendungen können mehrere Clients gleichzeitig bedienen.

## Com-Server

Kleine Endgeräte in [TCP/IP-Ethernet](#) Netzwerken, die Schnittstellen für serielle Geräte und digitale E/A-Punkte über das Netzwerk zur Verfügung stellen. Com-Server können sowohl als [Server](#) als auch als [Client](#) genutzt werden.

## DHCP - Dynamic Host Configuration Protocol

Dynamische, zeitlich begrenzte Zuteilung von [IP-Adressen](#) aus einem Adressenpool.

DHCP wird benutzt, um PCs in einem [TCP/IP](#)-Netz automatisch - also ohne manuellen Eingriff - zentral und somit einheitlich zu konfigurieren. Der Systemadministrator bestimmt, wie die IP-Adressen zu vergeben sind und legt fest, über welchen Zeitraum sie vergeben werden.

Grundsätzlich hat dieses Verfahren den Effekt, dass jeder Netzteilnehmer bei jeder neuen Verbindung eine andere IP-Adresse zugeteilt bekommt. Aus diesem Grund müssen Netzwerkkomponenten wie Com-Server oder Print-Server, die immer über eine festgelegte IP-Adresse angesprochen werden, von der IP-Adressenvergabe über DHCP ausgeschlossen werden.

DHCP ist in den Internet-Standards RFC 2131 (03/97) und RFC 2241 (11/97) definiert.

## DNS - Domain Name Service

Netzteilnehmer werden im [Internet](#) über numerische [IP-Adressen](#) angesprochen. Doch weil man sich Namen eben besser merken kann als Nummern, wurde der DNS eingeführt.

Wird vom Anwender zur Adressierung ein Domain-Name angegeben, erfragt der [TCP/IP-Stack](#) beim nächsten DNS-Server die zugehörige IP-Adresse. Im DNS-Server wird eine Liste geführt, in der die IP-Adressen des Netzwerkes, bzw. der Domäne, den entsprechenden Host-Namen zugeordnet sind.

Eine DNS-Tabelle kann folgendermaßen aussehen:

172.16.232.10 webthrm.firma.de

172.16.232.11 ntsrv.firma.de

172.16.232.12 novellsrv.firma.de

...

Wird nun durch eine Anwendung oder vom Benutzer z.B. der Teilnehmer "Ntsrv" verlangt, wird die Anfrage zunächst an den DNS-Server geschickt, der dann die IP-Adresse 172.16.232.11 für den Host-Namen zurückgibt. Im Internet funktioniert das Verfahren genauso. Die Internet DNS-Server enthalten allerdings Web-Adressen, z.B. klima.wut.de. Sollte der DNS-Server einen angefragten Host-Namen nicht in der Tabelle enthalten haben, so wird die Anfrage an benachbarte DNS-Server weitergereicht. Wenn nach einer bestimmten Zeit keine Antwort von einem DNS-Server erhalten wird, so wird die Verbindung abgebrochen und es erscheint im Web-Browser eine Fehlermeldung über die nicht gefundene Seite.

DNS beruht auf einem hierarchisch aufgebauten System: Jede Namensadresse wird über eine Top-Level-Domain ("de", "com", "net" usw.) und innerhalb dieser über eine Sub-Level-Domain identifiziert. Jede Sub-Level-Domain kann (muß aber nicht) nochmals untergeordnete Domains enthalten. Die einzelnen Teile dieser Namenshierarchie sind durch Punkte voneinander getrennt.

Netzwerkressourcen sollten sinnvollerweise einen Domain-Namen erhalten, der im Kontext zu der angebotenen Dienstleistung oder dem Firmennamen des Anbieters steht. So läßt sich z.B. "WuT.de" in die Top-Level-Domain "de" (= Deutschland) und die Sub-Level-Domain "WuT" (= Wiesemann & Theis GmbH) auflösen.

---

## DNS-Server

DNS-Server stellen im Internet die Dienstleistung zur Verfügung, einen Domain-Namen in eine IP-Adresse aufzulösen.

---

## Ethernet

Ethernet ist die zur Zeit bei lokalen Netzen am häufigsten angewandte Technologie. Es gibt drei verschiedene Ethernet Topologien: 10Base2, 10Base5 und 10BaseT; die Übertragungsrate beträgt 10 Mbit/s.

---

## Ethernet-Adresse

Die unveränderbare, physikalische Adresse einer Netzwerkkomponente im Ethernet.

---

## Firewall

Unter Firewall versteht man Netzwerkkomponenten, die ähnlich einem Router ein internes Netzwerk (Intranet) an ein öffentliches Netzwerk (z.B. Internet) anknüpfen. Hierbei lassen sich die Zugriffe ins jeweils andere Netz abhängig von der Zugriffsrichtung, dem benutzten Dienst sowie der Authentifizierung und Identifikation des Netzteilnehmers begrenzen oder komplett sperren.

Ein weiteres Leistungsmerkmal kann die Verschlüsselung von Daten sein, wenn z.B. das öffentliche Netz nur als Transitweg zwischen zwei räumlich getrennten Teilen eines Intranet genutzt wird.

---

## FTP - File Transfer Protocol

FTP ist ein auf TCP/IP aufsetzendes Protokoll, das es ermöglicht, ganze Dateien zwischen zwei Netzwerkteilnehmern zu übertragen. FTP arbeitet wie alle anderen Protokolle unter TCP nach dem Client-Server-Verfahren. Der FTP-Client übernimmt hierbei die Initiative, und der Anwender übergibt mit dem FTP-Kommando Parameter, die Art und Richtung der Datenübertragung bestimmen.

Nach dem Aufruf des FTP-Kommandos aus der DOS-Box

```
FTP <IP-Adresse des FTP-Servers>
```

wird zunächst die Verbindung zum FTP-Server aufgebaut, der dann seinerseits den Benutzernamen und ggf. ein Passwort erfragt.

Ist die Verbindung aufgebaut, kann durch Eingabe weiterer Befehle und Parameter auf den FTP-Server zugegriffen werden. Hier einige wichtige Befehle:

ascii schaltet auf die Übertragung von Text-Dateien um

binary schaltet auf die Übertragung von Binär-Dateien um

put <Dateiname> sendet die angegebene Datei an den FTP-Server

get <Dateiname> liest die angegebene Datei vom FTP-Server

Neben den hier aufgeführten Befehlen stellt FTP unter Windows eine Reihe weiterer Möglichkeiten zur Verfügung. Näheres kann man über die Hilfefunktion unter DOS erfahren (Eingabe des "?") am FTP Prompt). Die Syntax der FTP-Befehle unterscheidet sich allerdings von Betriebssystem zu Betriebssystem.

FTP ist in RFC 959 beschrieben.

---

## Gateway

Gateways verbinden - wie auch Bridges und Router - verschiedene Netze miteinander. Während Bridge und Router zwar ggf. die physikalische Art des Netzes umsetzen (z.B. Ethernet - ISDN), das eigentliche Protokoll (z.B. TCP/IP) aber unberührt lassen, bieten Gateways die Möglichkeit, einen Zugang zu protokollfremden Netzen zu schaffen (z.B. TCP/IP auf Profibus). Ein Gateway hat also unter anderem auch die Aufgabe, unterschiedliche Kommunikationsprotokolle zu übersetzen.

**Achtung:** bei der Netzwerkkonfiguration in Windows-Betriebssystemen wird auch die Eingabe eines Gateways gefordert. Diese Angabe bezieht sich allerdings auf einen ggf. im Netzwerk vorhandene Router!

---

## ICMP - Internet Control Message Protocol

Das ICMP-Protokoll dient der Übertragung von Statusinformationen und Fehlermeldungen zwischen IP-Netznoten. ICMP bietet außerdem die Möglichkeit einer Echo-Anforderung; auf diese Weise lässt sich feststellen, ob ein Bestimmungsort erreichbar ist.

vgl. auch Ping

---

## Internet

Das Internet ist der derzeit weltweit größte Netzverbund, der den angeschlossenen Netzteilnehmern eine nahezu grenzenlose Kommunikationsinfrastruktur zur Verfügung stellt. Durch Einsatz von TCP/IP können die Netzteilnehmer plattformunabhängig im Internet angebotene Dienste wie E-mail, FTP, Browser-Dienste wie HTTP usw. in Anspruch nehmen.

---

## Intranet

Ein abgeschlossenes Netzwerk (etwa innerhalb eines Unternehmens), in dessen Grenzen die Netzteilnehmer internetspezifische Dienste wie E-mail, FTP oder Browser-Dienste wie HTTP usw. in Anspruch nehmen können. In aller Regel gibt es von einem Intranet über Router bzw. Firewalls auch Übergänge in das Internet.

---

## IP - Internet Protocol

Protokoll, das die Verbindung von Teilnehmern ermöglicht, die in unterschiedlichen Netzwerken positioniert sind.

---

## IP-Adresse

Die IP-Adresse ist eine 32-Bit-Zahl, die jeden Netzteilnehmer im Internet bzw. Intranet eindeutig identifiziert. Sie besteht aus einem Netzwerkteil (Net-ID) und einem Benutzerteil (Host-ID).

---

## ISDN - Integrated Services Digital Network

ISDN ist der neue Standard in der Fernmeldetechnik und hat das analoge Fernsprechnetz in Deutschland komplett ersetzt. Bei ISDN werden Telefon und Telefax, aber auch Bildtelefonie und Datenübermittlung integriert. Über ISDN können also abhängig von den jeweiligen Endgeräten Sprache, Texte, Grafiken und andere Daten übertragen werden.

ISDN stellt über die S0 Schnittstelle eines Basisanschlusses zwei Basiskanäle (B-Kanäle) mit je 64 kbit/s sowie einen Steuerkanal (D-Kanal) mit 16 kbit/s zur Verfügung. Der digitale Teilnehmeranschluß hat zusammengefaßt eine maximale Übertragungsgeschwindigkeit von 144 kbit/s (2B+D). In den beiden B-Kanälen können gleichzeitig zwei unterschiedliche Dienste mit einer Bitrate von 64 kbit/s über eine Leitung bedient werden.

---

## ISDN-Router

ISDN-Router gestatten es, zwei lokale Netzwerke über das ISDN-Netz eines Telefonnetz-Providers miteinander zu verbinden. Dabei übernehmen ISDN-Router neben den normalen Funktionen eines Routers auch das Handling der ISDN-Verbindung.

---

## LAN - Local Area Network

Lokales Netz innerhalb eines begrenzten Gebiets unter Anwendung eines schnellen Übertragungsmediums wie z.B. Ethernet

---

## MAC-ID

Die unveränderbare, physikalische Adresse einer Netzwerkkomponente (MAC = Media Access Control).

vgl. auch Ethernet-Adresse

---

## NAT - Network Address Translation

Durch die explosionsartige Ausweitung des Internet in den letzten Jahren sind freie IP-Adressen knapp geworden und werden nur noch sehr sparsam vergeben. NAT kommt dort zum Einsatz, wo Firmennetze ans Internet angebunden werden. Das Firmennetz ist über einen NAT-fähigen Router mit dem Internet verbunden, arbeitet intern allerdings mit einem eigenen vom Internet unabhängigen IP-Adressraum. Von außen ist das Netz nur über eine einzige (oder einige wenige) IP-Adresse(n) ansprechbar. Anhand der Port-Nr. im empfangenen TCP/IP-Paket wird dieses an einen bestimmten internen Netzteilnehmer weiter geroutet.

Beispiel: Die Adresse klima.wut.de wird vom DNS-Server eines Providers aufgelöst und die Anfrage wird an die zugehörige IP-Adresse geschickt. Diese Anfrage kommt beim ISDN-Router an, der per NAT diese IP-Adresse auf die interne IP-Adresse des W&T Web-Thermometers umlenkt und so den Zugriff auf das Gerät ermöglicht.

---

## Ping - Packet Internet Groper

Ping dient in TCP/IP-Netzen zu Diagnosezwecken; mit Hilfe dieser Funktion läßt sich überprüfen, ob ein bestimmter Teilnehmer im Netz existiert und tatsächlich ansprechbar ist. Ping arbeitet mit dem ICMP-Protokoll, welches auf das IP-Protokoll aufsetzt. Setzt ein Netzteilnehmer durch Eingabe des Ping-Kommandos einen ICMP-Request ab, gibt die angesprochene Station einen ICMP-Reply an den Absender zurück. Der Aufruf des Kommandos PING <IP-Adresse> in der DOS-Box fordert den durch die IP-Adresse angegebenen Netzteilnehmer auf, eine Rückmeldung zu geben.

Zusätzlich können noch diverse Parameter angegeben werden:

-t Wiederholt das Ping-Kommando in Dauerschleife, bis der Anwender mit <Strg>C unterbricht.

-n count Wiederholt das Ping-Kommando "count" mal.

-l size "size" gibt an, mit wieviel Byte das ICMP-Paket aufgefüllt wird. Bei Com-Servern in Default-Einstellung sind dies maximal 512 Byte.

-w timeout "timeout" spezifiziert, wie lange (in Millisekunden) auf die Rückmeldung gewartet wird.

Beispiel:

```
PING 172.16.232.49 -n 50
```

wiederholt das Ping-Kommando an die Station 172.16.232.49 fünfzigmal.

Ist der Netzteilnehmer vorhanden, erscheint folgende Rückmeldung:

```
Reply from 172.16.232.49: bytes=32 time=10ms TTL=32
```

Bleibt die Rückmeldung aus, wird folgende Meldung zurückgegeben:

```
Request timed out.
```

Die von Ping verwendeten **ICMP**-Pakete sind im Internet-Standard RFC-792 definiert.

---

### PPP - Point to Point Protocol

PPP ist ein erweiterter Nachfolger von **SLIP** und weist u.a. eine verbesserte Fehlerkorrektur auf.

Genau wie SLIP bietet PPP die Möglichkeit, **TCP/IP**-Geräte, die keinen **LAN**-Anschluß haben, über die serielle Schnittstelle in TCP/IP-Netze einzubinden.

---

### RIP - Routing Information Protocol

Routing-Protokolle wie RIP dienen dazu, Veränderungen der Routen zwischen zwei vernetzten Systemen an die beteiligten Systeme weiterzuleiten und so eine dynamische Änderung der Routingtabellen zu ermöglichen.

RIP ist im Internet-Standard RFC-1058 definiert

---

### Router

Router verbinden zwei unterschiedliche Netze, wobei im Gegensatz zu Bridges nicht anhand der **Ethernet-Adresse**, sondern in Abhängigkeit von der **IP-Adresse** entschieden wird, welche Datenpakete weiterzuleiten sind.

vgl. auch [Bridge](#)

---

### Server

Anwendungen, welche Verbindungen von sogenannten **Clients** annehmen und die entsprechenden Dienste zur Verfügung stellen. Der bekannteste Server ist der Web-Server, welcher die Verbindungen von einem Web-Browser annimmt. Praktisch alle Internet-Dienste, wie Mail, **FTP**, **Telnet**, **Socket** usw. arbeiten nach dem **Client-Server** Schema.

Der Server wartet quasi auf "Anrufer", um diese bei Bedarf anzunehmen, während der Client der "Anrufer" ist.

---

### SLIP - Serial Line Internet Protocol

SLIP bietet eine einfache Möglichkeit zur Übertragung von **TCP/IP**-Datenpaketen über serielle Punkt-zu-Punkt-Verbindungen. Damit können Endgeräte, die nicht über einen **LAN**-Anschluß verfügen, auch über die serielle Schnittstelle ins Netzwerk eingebunden werden.

SLIP arbeitet nach einem sehr einfachen Algorithmus ohne eigene Datensicherungsverfahren: Dem eigentlichen IP-Datenpaket wird ein Startzeichen (dezimal 192) vorangestellt und ein Endzeichen (ebenfalls dezimal 192) angehängt. Um die binäre Transparenz zu erhalten, werden im Datenpaket vorkommende Start- und Endzeichen zuvor durch andere Sequenzen ersetzt.

SLIP ist in RFC 1055 beschrieben.

---

### SLIP-Router

Ein SLIP-Router stellt die Hardware und Funktionalität zur Verfügung, um serielle Endgeräte, die über einen **TCP/IP-Stack** verfügen, in ein Netzwerk einzubinden.

**Com-Server** stellen z.B. SLIP-Routing als Betriebsart zur Verfügung.

---

### SNMP - Simple Network Management Protocol

SNMP setzt auf **UDP** auf und ermöglicht die zentrale Administration und Überwachung von Netzwerkkomponenten.

SNMP ist in folgenden Standards spezifiziert: RFC 1052, RFC 1155, RFC 1156, RFC 1157, RFC 1213 und RFC 1441.

---

### Subnet-Mask

32-Bit-Wert, der festlegt, welcher Teil der **IP-Adresse** das Netzwerk und welcher den Netzwerkteilnehmer adressiert.

---

### TCP - Transmission Control Protocol

TCP setzt auf **IP** auf und sorgt nicht nur für die Verbindung der Teilnehmer während der Datenübertragung, sondern stellt auch die Korrektheit der Daten und die richtige Abfolge der Datenpakete sicher.

---

### TCP/IP-Stack

Teil des Betriebssystems oder ein auf das Betriebssystem aufgesetzter Treiber, der alle für die Unterstützung des **IP**-Protokolls benötigten Funktionen und Treiber zur Verfügung stellt.

---

### Telnet - Terminal over Network

In der Vergangenheit kam Telnet vor allem für den Fernzugriff über das Netzwerk auf UNIX-Sever zum Einsatz. Über eine Telnet-Anwendung (Telnet-Client) kann von einem beliebigen Rechner im Netz ein Fernzugriff auf einen anderen Rechner (Telnet-Server) erfolgen. Heute wird Telnet auch zur Konfiguration von Netzwerkkomponenten wie z.B. **Com-Servern** benutzt. Telnet wird unter **TCP/IP** normalerweise über Port-Nr. 23 angesprochen; für spezielle Anwendungen können aber auch andere Portnummern verwendet werden. Telnet setzt auf **TCP/IP** als Übertragungs- und Sicherheitsprotokoll auf.

Eigenschaften und Parameter von Telnet in der DOS-Box:

```
TELNET <IP-Adresse>  
baut eine Telnet-Verbindung auf den Port 23 des durch die IP-Adresse angegebenen Telnet-Servers auf.
```

```
TELNET <IP-Adresse> <Port-Nr>  
baut eine Telnetverbindung auf den angegebenen Port des adressierten Telnet-Servers auf.
```

Um z.B. eine Telnetverbindung auf den Konfigurations-Port (1111) eines W&T Com-Servers aufzubauen, könnte die Befehlszeile so aussehen:

```
TELNET 172.16.232.49 1111
```

In der Windows-Umgebung werden die Adressierungsparameter für Telnetverbindungen im Menü *Verbinden/Netzwerkssystem* eingegeben. Im Eingabefenster wird unter *Hostname* die IP-Adresse des Telnet-Servers, unter *Anschluß* die gewünschte Port-Nr. eintragen. Der vorgegebene Eintrag *telnet* entspricht Port 23.

Telnet ist im Internet-Standard RFC 854 definiert

---

### TFTP - Trivial File Transfer Protocol

Das Trivial File Transfer Protocol (TFTP) ist neben **FTP** ein weiteres Protokoll zur Übertragung ganzer Dateien. TFTP bietet nur ein Minimum an Kommandos, unterstützt keine aufwendigen Sicherheitsmechanismen und benutzt **UDP** als Übertragungsprotokoll. Da UDP ein ungesichertes Protokoll ist, wurden in TFTP eigene minimale Sicherungsmechanismen implementiert.

Das Trivial File Transfer Protocol ist in den Standards 783, 906, 1350 und 1782 bis 1785 beschrieben.

---

### UDP - User Datagram Protocol

UDP ist ein Protokoll, das wie **TCP** auf **IP** aufsetzt, im Gegensatz dazu aber verbindungslos arbeitet und über keine Sicherheitsmechanismen verfügt. Der Vorteil von UDP gegenüber TCP ist die höhere Übertragungsgeschwindigkeit.

Irrtum und Änderungen vorbehalten

---

Wir sind gerne persönlich für Sie da:

Wiesemann & Theis GmbH Porschestr. 12 42279 Wuppertal	Tel.: 0202/2680-110 (Mo-Fr. 8-17 Uhr) Fax: 0202/2680-265 info@wut.de
--	---

© Wiesemann & Theis GmbH, Irrtum und Änderungen vorbehalten; Da wir Fehler machen können, darf keine unserer Aussagen ungeprüft verwendet werden. Bitte melden Sie uns alle Ihnen bekannt gewordenen Irrtümer oder Missverständnisse, damit wir diese so schnell wie möglich erkennen und beseitigen können.

[Datenschutz](#)

